Governing Infrastructure as Code in Multi-Cloud Enterprises: Integrating Data Governance, MLOps, and Corporate Governance for Secure and Sustainable Digital Transformation

Alejandro M. Ríos
Universidad de los Andes, Colombia

Received: 11thNov 2025 |Received Revised Version: 25thNov 2025 | Accepted: 20th Dec 2025 | Published: 31th Dec 2025

Volume 07 Issue 12 2025

Abstract

The accelerating diffusion of multi-cloud strategies across large enterprises has radically transformed how digital infrastructures are designed, governed, and operated. At the heart of this transformation lies Infrastructure as Code (IaC), a paradigm that converts physical and virtual infrastructure into software-defined, version-controlled, and automatically deployed assets. While the technical efficiencies of IaC are now widely acknowledged, its governance, risk, compliance, and organizational implications remain theoretically underdeveloped and empirically fragmented. This article develops an integrated research framework that positions IaC as a central organizational control mechanism in multi-cloud ecosystems, linking it to data governance, MLOps, and corporate governance theory. Drawing on the best-practice architecture for enterprise multi-cloud deployments articulated by Dasari (2025), this study extends the concept of IaC beyond operational automation and situates it as a core instrument of institutional governance, risk mitigation, and strategic alignment.

The article synthesizes insights from contemporary data governance scholarship, MLOps pipeline research, and corporate governance theory to explain why IaC has become a pivotal governance technology in modern enterprises. From a data governance perspective, the article argues that IaC enables auditable, reproducible, and policy-enforced data infrastructures, thereby reducing data quality risks and legal exposure in highly regulated environments (Bernardo et al., 2024; Nag, 2024). From an MLOps perspective, IaC forms the infrastructural backbone of continuous machine learning pipelines, enabling controlled experimentation, reproducibility, and model lifecycle governance across heterogeneous cloud platforms (Google Cloud, 2024; Steidl et al., 2023). From a corporate governance perspective, IaC is theorized as a technological codification of organizational rules, analogous to governance codes that align managerial behavior with stakeholder interests (Aguilera & Cuervo-Cazurra, 2009; Larcker& Tayan, 2011).

Methodologically, this article adopts a theory-building design grounded in systematic literature integration and analytical synthesis. Rather than relying on statistical datasets, it constructs a conceptual model that connects multi-cloud complexity, infrastructural codification, and governance outcomes. The analysis demonstrates that enterprises adopting IaC in line with the architectural and procedural best practices identified by Dasari (2025) achieve superior transparency, reduced operational risk, and stronger alignment between IT execution and corporate governance objectives. The findings reveal that IaC does not merely automate infrastructure; it institutionalizes organizational intent into executable code, transforming governance from a human-centric compliance process into a continuous, machine-enforced system of control.

The discussion advances a new theoretical proposition: that IaC constitutes a form of "algorithmic governance" within the enterprise, bridging the gap between corporate governance codes and operational reality. This perspective explains why organizations with mature IaC capabilities are better positioned to manage regulatory compliance, data sovereignty, and ethical AI obligations in multi-cloud environments. The article concludes by outlining future research pathways for examining IaC as a governance institution, calling for empirical studies that link IaC maturity to financial performance, risk resilience, and organizational legitimacy.

Keywords:Infrastructure as Code, Multi-Cloud Governance, Data Governance, MLOps, Corporate Governance, Digital Transformation, Algorithmic Control

Cite This Article:Ríos, A. M. (2025). Governing Infrastructure as Code in Multi-Cloud Enterprises: Integrating Data Governance, MLOps, and Corporate Governance for Secure and Sustainable Digital Transformation. The American Journal of Engineering and Technology, 7(11), 258–265.

1. Introduction

The contemporary enterprise is increasingly defined by its dependence on digital infrastructure that spans multiple cloud providers, data platforms, and artificial intelligence systems. This environment, commonly described as a multi-cloud ecosystem, has emerged as the dominant organizational architecture for global corporations seeking flexibility, resilience, and competitive advantage (RightScale, 2024; Gartner, 2024). Yet this same architectural diversity has produced unprecedented complexity in how infrastructure is designed, deployed, and governed. What was once managed through centralized data centers and hierarchical IT departments is now distributed across programmable platforms that are updated continuously and often autonomously. Within this environment, Infrastructure as Code (IaC) has become a foundational mechanism for maintaining control, coherence, and accountability (Dasari, 2025).

IaC refers to the practice of defining and managing infrastructure through machine-readable code rather than manual configuration. Servers, networks, storage systems, and even security policies are specified in declarative or procedural scripts that can be versioned, tested, and deployed automatically across environments. In a multi-cloud context, where organizations operate simultaneously on platforms such as AWS, Azure, and Google Cloud, IaC provides a unifying layer of abstraction that standardizes how infrastructure is provisioned and maintained (Dasari, 2025). However, while the operational benefits of IaC have been widely documented, its deeper organizational implications remain insufficiently theorized.

From a governance perspective, enterprises face growing pressure to ensure that their digital infrastructures comply with regulatory, ethical, and strategic requirements. Data protection laws, financial regulations, and emerging AI governance frameworks impose obligations that extend far beyond technical uptime or cost efficiency (Nag, 2024; Bhaskaran, 2025). At the same time, corporate governance theory has long emphasized the need for mechanisms that align managerial decisions with stakeholder interests, mitigate agency problems, and ensure transparency (Aguilera et al., 2008; La Porta et al., 2000). Yet the digitalization of enterprise operations has outpaced the evolution of governance frameworks, leaving a gap between formal governance codes and the realities of algorithmically driven infrastructure.

It is within this gap that IaC acquires strategic significance. By translating organizational policies into executable code, IaC has the potential to become a new form of governance technology, one that enforces compliance, standardization, and accountability in real time. Dasari (2025) demonstrates that best-practice IaC architectures in multi-cloud enterprises incorporate security controls, auditability, and policy enforcement directly into deployment pipelines, thereby embedding governance into the technical fabric of the organization. This insight challenges the traditional view of governance as a primarily human-centered process and suggests a shift toward what may be described as algorithmic or infrastructural governance.

The relevance of this shift becomes even more pronounced when considering the role of data and artificial intelligence in contemporary enterprises. Data governance scholars have emphasized that data quality, lineage, and stewardship are essential for organizational innovation and legal compliance (Bernardo et al., 2024). Meanwhile, MLOps research has shown that continuous integration and deployment pipelines for machine learning models depend critically on stable, reproducible infrastructure (Steidl et al., 2023; Google Cloud, 2024). In multi-cloud environments, where data and models traverse heterogeneous platforms, the absence of standardized infrastructure governance creates risks of inconsistency, bias, and regulatory non-compliance. IaC, as articulated by Dasari (2025), offers a mechanism for harmonizing these diverse components into a coherent governance architecture.

Despite these developments, existing literature remains fragmented. Technical studies of IaC often focus on tooling and deployment efficiency, while governance research tends to address board structures, disclosure practices, and regulatory frameworks in isolation from digital infrastructure (Cuomo et al., 2016; Sheridan et al., 2006). Similarly, data governance and MLOps scholarship has yet to fully integrate the infrastructural dimension of multi-cloud operations. This fragmentation limits the ability of scholars and practitioners to understand how digital infrastructures can be governed in a manner consistent with corporate accountability, legal compliance, and ethical responsibility.

The present article addresses this gap by developing a comprehensive theoretical framework that connects IaC, data governance, MLOps, and corporate governance within multi-cloud enterprises. Building on the architectural and procedural insights provided by Dasari (2025), it argues that IaC should be understood not merely as a technical practice but as a central institutional mechanism that shapes organizational behavior. By embedding rules, standards, and controls into code, IaC transforms governance from an ex post auditing activity into a continuous, proactive system of enforcement.

This theoretical repositioning has far-reaching implications. If governance is increasingly encoded in infrastructure, then questions of corporate accountability, transparency, and stakeholder protection must be reexamined in light of technological design choices. The choice of how IaC templates are written, who controls their repositories, and how changes are reviewed becomes as consequential as board decisions or regulatory disclosures. In this sense, IaC functions analogously to corporate governance codes, which define acceptable practices and create expectations of behavior (Aguilera & Cuervo-Cazurra, 2009; Zattoni& Cuomo, 2008). Yet unlike traditional codes, IaC is executable, meaning that deviations are not merely discouraged but technically prevented.

The remainder of this article develops this argument in depth. The methodology section outlines the analytical approach used to integrate insights from diverse literatures into a coherent framework. The results section presents a conceptual model of IaC-based governance in multi-cloud environments, grounded in the best practices identified by Dasari (2025) and related scholarship. The discussion section offers a critical interpretation of these findings, situating them within broader debates about corporate governance, data ethics, and digital transformation. The conclusion reflects on the implications for theory, practice, and future research.

2. Methodology

The methodological foundation of this study is rooted in qualitative theory building through systematic literature integration and analytical synthesis. Rather than collecting primary empirical data, the research draws on an extensive body of peer-reviewed scholarship, practitioner frameworks, and policy-oriented analyses to construct a comprehensive conceptual model of Infrastructure as Code governance in multi-cloud enterprises. This approach is appropriate given the emergent and interdisciplinary nature of the phenomenon under investigation, which spans information systems, data governance, corporate governance, and organizational theory (Steidl et al., 2023; Aguilera et al., 2008).

The first methodological step involved the identification and prioritization of a core reference that provides authoritative guidance on IaC in multi-cloud environments. Dasari (2025) was selected as the anchor text because it offers a detailed, enterprise-level articulation of IaC best practices, explicitly addressing governance, security, and operational consistency across multiple cloud platforms. This reference was treated not as a prescriptive manual but as a theoretical lens through which broader governance issues could be examined. Its architectural principles, such as policy-as-code, version control, and automated compliance checks, were used as conceptual building blocks in the subsequent analysis.

The second step consisted of a systematic review of complementary literatures. Data governance and quality management research was examined to understand how organizations ensure the integrity, usability, and legality of their data assets (Bernardo et al., 2024; Nag, 2024). MLOps and AI pipeline scholarship was analyzed to capture how machine learning systems depend on stable and reproducible infrastructure (Google Cloud, 2024; Steidl et al., 2023; Floris &Alla, 2022). Corporate governance theory provided the institutional and organizational context, offering insights into how rules, incentives, and accountability structures shape managerial behavior (Larcker & Tayan, 2011; Aguilera & Cuervo-Cazurra, 2009; Filatotchev et al., 2013).

Rather than treating these literatures as independent domains, the methodology emphasized cross-domain synthesis. Concepts such as control, transparency, and accountability were traced across technical and organizational contexts to identify underlying commonalities. For example, the notion of "auditability" appears both in data governance, where it refers to traceable data lineage, and in corporate governance, where it denotes financial and operational oversight (Hermes et al., 2007; Bernardo et al., 2024).

IaC was theorized as a technological mechanism that operationalizes this shared requirement by making infrastructure changes traceable and reviewable through code repositories and deployment logs (Dasari, 2025).

Analytical coding was employed to categorize the functions of IaC described in the literature. These functions included standardization, automation, compliance enforcement, risk mitigation, and organizational learning. Each category was then mapped to corresponding governance outcomes, such as reduced agency costs, improved regulatory compliance, and enhanced strategic alignment (Aguilera et al., 2008; Morck et al., 2005). This mapping process allowed for the construction of a conceptual framework that links technical practices to institutional effects.

A critical dimension of the methodology was the incorporation of counter-arguments and alternative perspectives. Some scholars argue that excessive automation can lead to rigidity and loss of human judgment, potentially undermining governance rather than strengthening it (Cuomo et al., 2016; Nowland, 2008). These concerns were integrated into the analysis to ensure that the framework did not present IaC as a panacea but rather as a contested and evolving governance technology. The methodology therefore remained interpretive and reflexive, acknowledging the limitations and uncertainties inherent in theorizing about rapidly changing digital infrastructures.

The study also drew on maturity model concepts from software engineering and organizational research to situate IaC adoption within broader trajectories of organizational development (Garcia et al., 2007). This allowed for the differentiation between superficial adoption of IaC tools and deeper institutionalization of IaC as a governance mechanism. Enterprises at lower levels of maturity may use IaC merely to speed up deployments, while more mature organizations integrate it into risk management, compliance, and strategic planning processes (Dasari, 2025).

In terms of rigor, the methodological approach sought to ensure conceptual coherence and theoretical plausibility rather than statistical generalizability. The validity of the framework rests on the consistency of its interpretations with established theories and empirical observations reported in the literature. By grounding the analysis in multiple, independently validated sources, the study mitigates the risk of idiosyncratic or biased conclusions (Aguilera & Cuervo-Cazurra, 2009; Steidl et al., 2023).

Limitations of this methodology must also be acknowledged. The reliance on secondary sources means that the framework cannot capture the full diversity of organizational practices or the dynamic evolution of technologies in real time. Furthermore, the integration of technical and governance literatures involves interpretive judgments that may be contested by specialists in either domain. Nevertheless, given the exploratory and theory-building nature of the research question, this approach provides a robust foundation for advancing scholarly understanding of IaC governance in multi-cloud enterprises.

3. Results

The analytical synthesis of the literature reveals a coherent pattern: Infrastructure as Code operates as a central governance mechanism in multi-cloud enterprises by translating organizational policies into enforceable technical rules. This finding aligns with the architectural principles articulated by Dasari (2025), who demonstrates that IaC frameworks in large organizations are designed not merely to automate deployment but to embed security, compliance, and standardization directly into the infrastructure lifecycle. When viewed through the lens of corporate and data governance theory, this technical architecture produces a set of institutional effects that fundamentally reshape how organizations control and coordinate their digital operations.

One of the most significant results is the identification of IaC as a mechanism of standardization across heterogeneous cloud environments. Multi-cloud strategies are often adopted to avoid vendor lock-in and to leverage the unique capabilities of different providers, but this diversity also creates risks of fragmentation and inconsistency (Gartner, 2024). Dasari (2025) shows that IaC templates act as a unifying grammar that ensures infrastructure components are provisioned according to the same rules, regardless of the underlying platform. From a governance perspective, this standardization reduces the discretion of individual administrators and aligns operational practices with centrally defined policies, thereby lowering agency costs and enhancing organizational coherence (Aguilera et al., 2008).

A second key result concerns auditability and traceability. In traditional IT environments, infrastructure changes were often undocumented or recorded in disparate systems, making it difficult to reconstruct decision histories or assign responsibility (Sheridan et al., 2006). By contrast, IaC requires that all changes be committed to version-controlled repositories, creating a permanent and reviewable record of who made what change and why (Dasari, 2025). This technical traceability mirrors the disclosure and transparency requirements emphasized in corporate governance codes, which seek to provide stakeholders with reliable information about organizational actions (Nowland, 2008; Aguilera & Cuervo-Cazurra, 2009). The result is a convergence between technical and institutional forms of accountability.

The integration of IaC with data governance frameworks represents another critical outcome. Bernardo et al. (2024) emphasize that data quality and governance depend on consistent processes for data collection, storage, and access. In multi-cloud environments, where data may be replicated across platforms and jurisdictions, these processes are particularly vulnerable to breakdowns. Dasari (2025) demonstrates that IaC can enforce data-related policies, such as encryption standards and access controls, at the infrastructure level. This means that data governance is no longer dependent solely on human compliance but is embedded in the technical fabric of the organization, reducing the risk of inadvertent or malicious violations (Nag, 2024).

The results also highlight the role of IaC in supporting MLOps and AI governance. Continuous machine learning pipelines require stable, reproducible infrastructure to ensure that models can be trained, tested, and deployed in a controlled manner (Steidl et al., 2023; Google Cloud, 2024). IaC provides this stability by ensuring that environments are identical across development, testing, and production. Dasari (2025) notes that enterprises using IaC can recreate entire ML environments on demand, facilitating debugging, auditing, and regulatory review. From a governance standpoint, this capability is crucial for addressing concerns about algorithmic bias, model drift, and accountability in AI systems (Bhaskaran, 2025; Nag, 2024).

Another important result is the emergence of what may be termed “policy-as-code.” In advanced IaC implementations, organizational rules regarding security, cost management, and compliance are expressed in machine-readable policies that are evaluated automatically during deployment (Dasari, 2025). This approach parallels the function of corporate governance codes, which articulate standards of good practice and provide benchmarks for evaluation (Cuomo et al., 2016; Zattoni& Cuomo, 2008). The difference is that policy-as-code is enforced in real time, preventing non-compliant configurations from being deployed at all. This shifts governance from an ex post to an ex ante mode, fundamentally altering the temporal dynamics of control.

Finally, the results indicate that the governance impact of IaC depends on organizational maturity. Drawing on maturity model theory (Garcia et al., 2007), it becomes clear that enterprises at early stages of IaC adoption may achieve operational efficiencies without realizing full governance benefits. Only when IaC is integrated into formal risk management, compliance, and strategic planning processes does it become a true governance technology (Dasari, 2025). This finding underscores the importance of institutional context in shaping the outcomes of technical innovations, echoing insights from corporate governance research about the role of national and organizational institutions (Filatotchev et al., 2013; Hermes et al., 2007).

4. Discussion

The results presented above invite a profound rethinking of how governance operates in digitally mediated organizations. Traditionally, corporate governance has been conceptualized as a system of formal rules, board structures, and regulatory frameworks designed to align managerial behavior with stakeholder interests (Larcker & Tayan, 2011; La Porta et al., 2000). In parallel, data governance and IT governance have been treated as specialized domains concerned with information quality, security, and compliance (Bernardo et al., 2024; Nag, 2024). The emergence of Infrastructure as Code in multi-cloud enterprises collapses these distinctions by embedding governance directly into the operational infrastructure, creating what may be described as a regime of algorithmic governance (Dasari, 2025).

From a theoretical perspective, this development resonates with institutional theories that emphasize the role of formalized rules and routines in shaping organizational behavior (Aguilera et al., 2008; Filatotchev et al., 2013). IaC templates and policies function as institutionalized scripts that define what actions are possible and permissible within the organization. Unlike traditional policies, however, these scripts are executed automatically by machines, leaving little room for discretionary deviation. This raises both opportunities and challenges. On the one hand, the reduction of human discretion can mitigate agency problems, opportunism, and error, leading to more reliable and transparent operations (Morck et al., 2005; Dasari, 2025). On the other hand, it risks creating rigid systems that may fail to adapt to novel situations or ethical dilemmas not anticipated by their designers (Cuomo et al., 2016).

The integration of IaC with data governance further amplifies these dynamics. Bernardo et al. (2024) argue that effective data governance requires not only formal policies but also technical mechanisms that ensure data quality and traceability. IaC provides such mechanisms by enforcing consistent infrastructure configurations across environments, thereby reducing the likelihood of data corruption or unauthorized access. Yet this technical enforcement also raises questions about accountability. If a data breach occurs because of a flawed IaC template, who is responsible: the developer who wrote the code, the manager who approved it, or the organization as a whole? Corporate governance theory has long grappled with similar issues in the context of financial reporting and internal controls (Aguilera & Cuervo-Cazurra, 2009; Nowland, 2008), suggesting that new frameworks will be needed to allocate responsibility in algorithmically governed systems.

MLOps and AI governance provide an especially revealing lens through which to examine these issues. Steidl et al. (2023) and Google Cloud (2024) emphasize that continuous delivery pipelines for machine learning models depend on reproducible and auditable infrastructure. IaC makes such reproducibility possible, enabling organizations to demonstrate how a particular model was trained and deployed. This capability is increasingly important as regulators and the public demand greater transparency and fairness in AI systems (Bhaskaran, 2025; Nag, 2024). At the same time, the automation of model deployment through IaC raises concerns about the speed and scale at which potentially harmful algorithms can be propagated. Here again, the tension between efficiency and control becomes apparent, echoing long-standing debates in corporate governance about the trade-offs between managerial autonomy and oversight (Larcker&Tayan, 2011; Zattoni& Cuomo, 2008).

Comparative corporate governance research also sheds light on the institutional variability of IaC adoption. Filatotchev et al. (2013) and Hermes et al. (2007) show that governance practices are shaped by national legal systems, cultural norms, and economic structures. In the context of IaC, this suggests that the same technical tools may produce different governance outcomes in different institutional environments. For example, enterprises operating in jurisdictions with strict data protection laws may use IaC to enforce rigorous compliance, while those in more permissive environments may prioritize cost efficiency and speed. Dasari (2025) implicitly acknowledges this variability by emphasizing the need for customizable policy frameworks within IaC architectures.

A further dimension of the discussion concerns the relationship between IaC and organizational learning. Garcia et al. (2007) argue that maturity models reflect not only technical capabilities but also the institutionalization of best practices. As enterprises progress in their IaC maturity, they accumulate knowledge about what configurations work best, how risks can be mitigated, and how governance objectives can be achieved. This learning is encoded in IaC repositories, creating a form of organizational memory that persists beyond individual employees. Such memory enhances resilience and continuity, key objectives of corporate governance (Aguilera et al., 2008; Morck et al., 2005).

However, the concentration of governance power in code repositories also introduces new vulnerabilities. If IaC templates are compromised, misconfigured, or controlled by a small group of insiders, the entire organization may be exposed to systemic risk (Dasari, 2025; Bhaskaran, 2025). This mirrors concerns in corporate governance about the concentration of power and the need for checks and balances (La Porta et al., 2000; Aguilera & Cuervo-Cazurra, 2009). Effective IaC governance therefore requires not only technical controls but also organizational processes for review, approval, and oversight, such as code audits, segregation of duties, and independent verification.

The broader implication of these findings is that digital transformation is inseparable from governance transformation. As enterprises migrate to multi-cloud architectures and adopt IaC, they are not merely changing how they deploy servers or applications; they are redefining how authority, accountability, and control are exercised. Dasari (2025) provides a technical blueprint for this transformation, but its organizational consequences extend far beyond the IT department. Boards of directors, regulators, and stakeholders must come to terms with the fact that governance is increasingly enacted through algorithms and infrastructure rather than solely through human decision-making.

Future research should build on this insight by empirically examining how IaC maturity correlates with governance outcomes such as financial performance, regulatory compliance, and stakeholder trust. Comparative studies across industries and jurisdictions could illuminate how institutional contexts shape the adoption and impact of IaC-based governance. Additionally, normative research is needed to address ethical questions about algorithmic control, transparency, and accountability in digitally governed organizations (Nag, 2024; Bhaskaran, 2025). By situating IaC at the intersection of technology and governance, scholars can develop more holistic theories of the modern enterprise.

5. Conclusion

This article has argued that Infrastructure as Code is not merely a technical innovation but a foundational governance mechanism in multi-cloud enterprises. Drawing on the best-practice framework articulated by Dasari (2025) and integrating insights from data governance, MLOps, and corporate governance scholarship, it has shown how IaC embeds organizational rules into executable infrastructure, transforming how control, accountability, and compliance are achieved. In doing so, IaC bridges the gap between abstract governance codes and the operational realities of digital organizations.

The theoretical framework developed here suggests that enterprises with mature IaC capabilities are better positioned to manage the complexities of multi-cloud environments, mitigate risks associated with data and AI, and align their technological operations with broader stakeholder expectations. At the same time, the rise of algorithmic governance raises new challenges regarding responsibility, transparency, and institutional oversight. Addressing these challenges will require not only technical innovation but also the evolution of governance theories and practices.

As digital infrastructures continue to expand in scope and importance, understanding IaC as a governance institution will become increasingly critical. By recognizing the political and organizational dimensions of code, scholars and practitioners alike can contribute to the development of more accountable, resilient, and ethically grounded enterprises.

References

1. Bhaskaran, S. B. (2025). Securing the future: How big data can solve the data privacy paradox. Forbes Technology Council.
2. Aguilera, R. V., Filatotchev, I., Gospel, H., & Jackson, G. (2008). An organizational approach to comparative corporate governance: Costs, contingencies, and complementarities. Organization Science, 19(3), 475–492.
3. Google Cloud. (2024). MLOps: Continuous delivery and automation pipelines in machine learning. Cloud Architecture Center.
4. Hermes, N., Postma, T. J. B. M., & Zivkov, O. (2007). Corporate governance codes and their contents: An analysis of Eastern European codes. Journal of East European Management Studies, 12(1), 53–74.
5. Garcia, V. C., Lucrédio, D., Alvaro, A., de Almeida, E. S., de Mattos Fortes, R. P., & de Lemos Meira, S. R. (2007). Towards a maturity model for a reuse incremental adoption. SimpósioBrasileiro de Componentes, Arquiteturas e Reutilização de Software.
6. Larcker, D., & Tayan, B. (2011). Corporate governance matters: A closer look at organizational choices and their consequences. Pearson Education.
7. Dasari, H. (2025). Infrastructure as code (IaC) best practices for multi-cloud deployments in enterprises. International Journal of Networks and Security, 5(1), 174–186. https://doi.org/10.55640/ijns-05-01-10
8. Bernardo, B. M. V., São Mamede, H., Barroso, J. M. P., & dos Santos, V. M. P. D. (2024). Data governance & quality management—Innovation and breakthroughs across different fields. Journal of Innovation & Knowledge, 9(4), 100598.
9. Aguilera, R. V., & Cuervo-Cazurra, A. (2009). Codes of good governance. Corporate Governance: An International Review, 17(3), 376–387.
10. Steidl, M., Felderer, M., & Ramler, R. (2023). The pipeline for the continuous development of artificial intelligence models—Current state of

research and practice. Journal of Systems and Software, 199, 111615.

11. Zattoni, A., & Cuomo, F. (2008). Why adopt codes of good governance? A comparison of institutional and efficiency perspectives. Corporate Governance: An International Review, 16(1), 1–15.

12. Floris, S., &Alla, S. (2022). Orchestration for data, machine learning, and infrastructure. Union.

13. La Porta, R., Lopez-de-Silanes, F., Shleifer, A., &Vishny, R. W. (2000). Investor protection and corporate governance. Journal of Financial Economics, 58(1), 3–27.

14. Cuomo, F., Mallin, C., &Zattoni, A. (2016). Corporate governance codes: A review and research agenda. Corporate Governance: An International Review, 24(3), 222–241.

15. Morck, R., Wolfenzon, D., & Yeung, B. (2005). Corporate governance, economic entrenchment and growth. Journal of Economic Literature, 43, 655–720.

16. Nag, D. (2024). AI technologies and the data governance framework: Navigating legal implications. Dataversity.

17. Nowland, J. (2008). The effect of national governance codes on firm disclosure practices: Evidence from analyst earnings forecasts. Corporate Governance: An International Review, 16(6), 475–491.

18. Sheridan, L., Jones, E., & Marston, C. (2006). Corporate governance codes in the supply of corporate information in the UK. Corporate Governance: An International Review, 14(5), 475–491.

19. Balaskas, G., Papadopoulos, H., Pappa, D., Loisel, Q., & Chastin, S. (2025). A framework for domain-specific dataset creation and adaptation of large language models. Computers, 14(5), 172.

20. Müller-Stewens, G., & Lechner, C. (2005). Strategisches Management. Schäffer-Poeschel.